SYSTEM AND METHOD FOR SECURING USING DECRYPTION KEYS DURING FPGA CONFIGURATION USING A MICROCONTROLLER

ABSTRACT

A system for securely using decryption keys during FPGA configuration includes a FPGA having a microcontroller for receiving a bitstream having an encrypted bitstream portion as well as a configuration boot program. The configuration boot program can be code that runs on an embedded hardware microcontroller or a software microcontroller. The system further includes a key storage register coupled to the microcontroller for storing key data from the microcontroller, a decryptor coupled to the key storage register, and a configuration data register in the FPGA. Preferably, only the decryptor can read from the key storage register and the configuration data register cannot be read by the microcontroller after the decryptor is used.